



March 8, 2019

BSA COMMENTS ON THE INTERIM REPORT FROM THE STUDY GROUP ON PLATFORM SERVICES

General Comments

Chapter 1: Background of the Study on Securing the Handling of User Information in Line with the Expansion of Platform Services

BSA | The Software Alliance (BSA)¹ appreciates the opportunity to provide feedback in response to the consultation by the Ministry of Internal Affairs and Communications (MIC) on the Interim Report from the Study Group on Platform Service (Interim Report). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things (IoT). BSA members have made significant investments in Japan and are proud that many Japanese organizations and consumers continue to benefit from BSA member products and services supporting Japan's economy.

BSA thus has a significant interest in the Interim Report and its potential impact on BSA members and the technology sector in general. Although we appreciate the efforts by MIC to enhance the regulatory framework for digital platform services to ensure user protection, we are concerned that some of the Interim Report's preliminary recommendations could undermine this objective and result in negative effects on the wider digital economy in Japan. Several of the Interim Report's preliminary recommendations are ambiguous. It is unclear, for instance, what scope of platform services would fall under the recommended extra-territorial application designed to provide stricter protection on secrecy of communication. Applying such regulation without clarity on the intended business operators would not result in building a workable system and will be difficult to implement, creating confusion for many service providers operating globally. Such a policy creates a risk of international fragmentation and the potential for other countries to impose their own laws extra-territorially on Japanese companies. The broader and stricter application of Japan's concept and approach to protect secrecy of communication would run counter to MIC's intent to maintain international interoperability or harmonization of legal regimes affecting digital trade. Such confusion will not support achieving user protection and could also bring unintended consequences on cybersecurity as well as impede innovation.

In our experience, policy frameworks are most effective when they are proportionate, principles-based, outcomes-focused, and not unduly prescriptive. As detailed in BSA's Global Privacy Best Practices (Best Practices),² we support the implementation of privacy and data protection policies that increase the transparency of personal data collection and use; enable and respect informed

¹ BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

² At: https://www.bsa.org/~media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdf

choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes. With respect to territoriality, BSA advocates for data protection frameworks that govern conduct only where: (1) residents are specifically targeted, (2) the personal data that is the object of the processing is purposefully collected from data subjects in the country at the time of collection, and (3) such collection is performed by an entity established in the country through a stable arrangement giving rise to a real and effective level of activity. We recommend that the Interim Report's recommendations should be reconsidered with these principles in mind and urge further engagement with relevant stakeholders.

Recommendations

Based on the above, we offer specific comments on Interim Report below:

Chapter 3/Section 2

Major Points of Discussion and Basic Direction Regarding Policy Measures Related to Various Items Under Review

The Interim Report recommends reviewing and revising the Telecommunications Business Act (TBA)³ and related guidelines to protect users. Japan has largely taken a principles-based, outcomes-focused approach to privacy and data protection, primarily through its Act on the Protection of Personal Information (APPI).⁴ Introducing amendments to the TBA of the type that the Interim Report appears to envisage and even more prescriptive requirements via related guidelines would significantly compromise the effectiveness of the current legal regime for protection personal information and consumer privacy in Japan. This could create uncertainty that would undermine innovation and the development of the digital economy in Japan. Japan already has an established legal system for the protection of personal information which stipulates personal information is to be used within the scope of purpose presented to users, requiring entities to manage personal information in an open and transparent way, while having a clearly-expressed and up-to-date privacy policy. As the implementation of APPI is under the supervision of the Personal Information Protection Commission (PPC), which is entitled to take action against disclosures or breaches by business operators located outside of Japan, the issues articulated in the Interim Report should be resolved under the framework of APPI. Given the PPC's continued dialogue with relevant overseas stakeholders, including enforcement authorities, PPC is in a strong position to ensure the protection and utilization of personal information in Japan and maintain international interoperability with other personal data protection legal regimes. Having a dual regulation with two administrative agencies authorized to enforce against foreign business operators will remove the significance of the PPC as the central, independent authority on privacy, creating confusion for many operators providing services to users in Japan.

If, after appropriate inquiry and consultation, MIC considers that any additional guidance is required as to what is reasonable in specific circumstances, this guidance should be developed and implemented in accordance with existing system for personal information protection, rather than via the introduction of another layer of prescriptive requirements. It is also important that any such guidance continue to preserve existing flexibility in business operations.

³ Telecommunications Business Act at: http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=359AC0000000086
English translation at: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf

⁴ Act on the Protection of Personal Information at: https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf
.English translation at: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

The Government of Japan seeks to support and enable the creation of new businesses utilizing advanced technology to advance Society 5.0. The introduction of excessive and duplicative regulations will interfere with this objective, slowing Japan's economic growth, and impeding innovation especially among Japan's SMEs and startups. The notion of "platforms" in the Interim Report is expansive. The business models of "digital platformers" vary significantly between business operators, and deeper discussions and deliberation on the design structure of any further recommendations should be held based on a clear understanding of the differences in their businesses. Given that each business operator has initiatives underway according to their business model for protecting their users' information, MIC should fully take into account the effectiveness of voluntary industry initiatives when considering any further regulations.

Chapter 2/Section 1

Legal Systems Related to the Handling of User Information in the Fields of Telecommunications

The Interim Report explains the protection on secrecy of communication under the TBA and examples of conduct that would be considered in violation of secrecy of communication, including obtaining knowledge and use of user information without permission. Considering the significant advancement of technology since the TBA was enacted, regulation that designed to protect users is now presenting challenges to ensuring cybersecurity. The TBA limits the ability to share information among stakeholders upon the discovery of malware. Specifically, when software companies discover infected computers from malicious transmissions and stand ready to share information with network operators to shut down further harmful transmissions in a timely manner, the network operators face difficulty in recording, checking, and analyzing log data due to concerns about violating the secrecy of communications of their users. Treating communications and meta data in the same way can therefore lead to harmful results by delaying the timely sharing of relevant information in order to respond to an emerging cybersecurity incident. We encourage MIC to treat transmission log information and related metadata differently from the content of communications. By clarifying for domestic network operators that there would not be a violation of the secrecy of communication requirements of the TBA in such circumstances, amendments to the TBA could enhance the ability of business operators in various fields to share digital evidence and work together to ensure the safety of users. Therefore, MIC's review of the TBA should be focused not only on whether protecting user information, but also on enhancing cybersecurity capabilities in Japan.

C. Conclusion

Chapter 6: Procedure for Future Studies

The above are BSA's preliminary observations. Given the ambiguity and complexity of the Interim Report, we encourage MIC to further explore the issues in depth before concluding the discussion and respectfully encourage MIC to engage in further dialogue with industry to consider the broader issues at play and the implications of the recommendations made in the Interim Report.

For Japan to take a leading role in privacy protection while enabling digital trade and economic growth and development, it is critical to achieve international interoperability among the various personal information protection regimes globally. It is therefore important that issues raised in the Interim Report are discussed under the implementation framework of APPI.

We hope this submission will be helpful in developing and delivering other enduring solutions to address the challenges related to the regulation of digital platforms. In the future, we would very much appreciate if MIC could allow a longer period for public consultation and such matters. It was very difficult to translate and sufficiently evaluate the content of the Interim Report and

develop thoughtful and constructive input in such a short period of time. Given that the Interim Report directly addresses how international firms interact with Japan's legal and regulatory system, it would be preferable to provide an adequate period of time to respond to further developments in this area in the future.

We look forward to working with MIC in the future and welcome the opportunity to exchange views.